OTA
Online Trust Alliance

Via electronic email

October 15, 2010

Chairman Julius Genachowski
Federal Communications Commission
445 12th Street SW
Washington, DC 20554

Re: Federal Communications Commission
Creation of a Cybersecurity Roadmap / National Broadband Plan - Request for Comments
PS Docket No. 10-146
GN Docket No. 09-51

Dear Chairman Julius Genachowski,

The Online Trust Alliance (OTA) hereby submits its comments to your Request for Comments regarding the creation of a National Broadband Cybersecurity roadmap. We look forward to meeting with your staff on October 19th to discuss this submission in more detail.

OTA is in full agreement with the Commission's statement that the "lack of trust in online experiences will quell demand for broadband services and left unchecked the current and anticipated vulnerabilities in the communication infrastructure could threaten life safety and privacy". OTA suggests these threats are already in play and causing quantifiable harm today. Trust is the foundation of every interaction on the internet. Left unchecked, these threats will continue to impact the growth of commerce, resiliency of our infrastructure and national security.

OTA was founded in 2004 to address the global spam problem and the lack of standards to help detect forged email. Over the past six years, OTA has grown significantly. As an IRS approved 501(c)(6) member- based non-profit, we represent the broad internet ecosystem and are not beholden to any special interest or trade group. OTA is comprised of businesses, government bodies and NGOs who share our mission to protect the vitality, trust and confidence of the internet.

Core to OTA's mission is the protection of users' online trust and confidence that we believe are the foundation of the internet economy and therefore require active protection. This requires a renewed focus and collaboration between the public and private sectors. To succeed will require a combination of investments, incentives and a willingness to change business practices as the onslaught of cybercrime continues to tarnish online trust.

As the use of alternative devices including smartphone, mobile devices and tablets proliferates, a comprehensive device agnostic cybersecurity strategy is essential. Mobile devices contain vast amounts of personal and business confidential data and are increasingly being exploited. Methods to protect such data including encryption, remote wiping and other services need to become standard consumer offers and practices from device manufacturers and carriers. As these devices have become prevalent and at times the primary connectivity to the internet, carriers need to provide users added security and privacy capabilities and user controls. With geo-location services rapidly emerging, the implications to security and privacy as well as personal safety are significant. Providing user controlled policy setting capability to opt out of certain types of services or websites should be part of a service provider's standard service offering. Users must be afforded choice and controls over the collection and sharing of their data as well as the ability to block email and text messages from unsolicited sources. Combined these controls provide consumers enhanced control of the data usage, privacy and security and long term will help encourage their usage of mobile services.

We believe that all stakeholders have a shared responsibility in curbing these threats. Businesses, infrastructure providers, carriers, ISPs, web publishers and the interactive advertising supply chain all need to work to help counter this abuse. Concurrently, consumers need to practice safe computing and follow the recommendations of Stop, Think and Connect.[1] Users need to exercise caution when downloading documents, video and other files from unknown publishers and sources. Not unlike having to drive defensively and maintain a safe vehicle on the highway, users need to take reasonable steps in patching vulnerabilities and using anti-virus and malware services to help protect their computers from these threats. While there is no silver bullet, working together we can reduce the attack surface and increase the "cost of doing business" to the cybercriminal, creating an economic disincentive.

While the scope of this document is focused on cybersecurity, we recommend that the Commission look at the continuum of threats including the convergence of data stewardship, privacy and security. Looking at each in isolation, may be unproductive and potentially damaging the goal of restoring and protecting online trust.

Specific to your request for comments, we have outlined the following;

1. Legislation & Regulation – The role of government is essential for effective cybersecurity and protection of critical infrastructure. However a unified approach that reconciles the various efforts within government and the private sector must be established. Navigating the labyrinth of cybersecurity, data governance and privacy legislation overseen by multiple regulatory agencies can be overwhelming. The challenge is to not adversely impact legitimate and responsible businesses that are faced with jurisdictional questions and overlapping areas of responsibility. To be effective and to encourage innovation and economic prosperity, any such regulations must be aligned. As collaboration and data sharing is a key component in the fight against the cybercriminal, existing and new regulations need to encourage data sharing and collaboration with law enforcement. Fundamentally OTA believes in self-regulation and market based incentives. OTA is committed to working across the ecosystem to support such efforts in tandem with balanced and effective legislation.

[1] National Cybersecurity Consumer Awareness Campaign, www.onguardonline.gov

2. Responsibility & Stewardship of Infrastructure Providers - Internet Service Providers (ISP) and mobile carriers play an important role in the security, privacy and governance of the internet. While dealing with attacks on their infrastructure they must also take proactive steps to protect users. Unfortunately in many communities consumers have limited broadband choices. It can be difficult for them to change providers even if they desire more secure services, anti-spam technologies or consumer oriented privacy and data sharing practices. As with privacy policies of web sites, the policies and practices of broadband providers are often difficult for users to discover, comprehend or compare from between one ISP or carrier and another. We believe the FCC should facilitate voluntary steps and encourage best practices including:

    a. Establishment of an ISP / Carrier Safety Rating - Not unlike a health department rating of a restaurant, or the National Highway Traffic Safety Administration vehicle crash tests, such ratings could provide transparency for consumers and a means of comparing security and privacy services and policies, based on defined and measurable criteria.[2] This could increase security and privacy competition and could allow consumers to changes their ISP or carrier without penalties should they fail to provide reasonable security. In addition to cancelation penalties which should be waived in the case of security breaches, a major limitation to consumers making a change to another provider is the portability of their email addresses. Portability solutions such as "no-charge" mail forwarding should be considered for a minimum period to provide consumers added freedom to select their broadband provider.
    b. Email Authentication - Spam, forged and spoofed email continues to compromise consumers. While email authentication is a recognized best practice, broader support is required. Today only 60% of the top 100 financial services companies and 58% of the Internet Retail 500 are using authentication to help protect consumers and brands from deceptive email. Additionally, only 40% of the top consumer-facing U.S. Government agencies have adopted one or more email authentication standards. Email authentication is now included in the draft National Strategy for Trusted Identities in Cyberspace (NSTIC), to help protect citizens as well as Federal employees from malware, bots and key loggers.[3] While supported by the White House and FTC, the FCC, has yet to adopt email authentication.[4] Broadband providers should be encouraged to adopt inbound authentication as part of their anti-spam arsenal.

3. Protection of Trusted Web Properties – Over the past three years the percent threats to web site infrastructure have increased over 600%.[5] Cybercriminals have evolved to targeting trusted web sites and the online advertising infrastructure. In the absence of integrated controls, standards and end-to-end accountability, these intrusions have been flourishing. "Malvertising" offers the ability to for the cybercriminal to remain anonymous with expansive malware distribution capabilities. OTA has recently released best practices to help curb this evolving threat.[6] We look to coordinated government support for these and other efforts to help stem this consumer threat.

[2] http://www.safercar.gov/

[3] https://otalliance.org/resources/authentication/index.html

[4] To support the FCC's adoption of email authentication, OTA will provide resources and assistance.

[5] Source: 2010 Symantec & Microsoft Security Intelligence Reports

[6] https://otalliance.org/resources/malvertising.html

OTA believes ISPs can take a more active role in the detection and remediation of these web based threats. A growing number of ISP and transit providers have the capabilities, yet their use is encumbered by privacy and legal concerns. Creating a safe harbor for data sharing and reporting could help alleviate these concerns allowing deep packet inspection at the header level, with verifiable privacy protections. At the same time protections must be firmly established to prevent abuse or the monetization of such data as attempted by major broadband providers.[7]

4. Consumer & Business Education -Technology alone cannot counter all of the threats on the Internet. User education is required to reduce the number of at-risk PCs and to instill safe browsing practices. This need is not limited to consumers, but also to business users. We applaud efforts such as the recent Stop, Think and Connect campaign to help educate consumers to cyber security risks. At the same time, we are concerned that too much reliance is being placed on broad-reach awareness initiatives. OTA believes the equivalent if not greater resources and incentives should be allocated remedial efforts and solution oriented teachable moments. For example, ISP's could be incentivized or encouraged to scan user systems for out of date browsers or vulnerable ad- ons and proactively direct users to patch their systems. Systems that do not pass could either be put into a quarantine network with limited external access or possibly denied internet access. Such approaches need to be balanced by the implications to privacy as well as the potential financial costs of supporting such initiatives.

5. Extended Validation SSL Certificates - EV SSL Certificates are currently deployed by over 30,000 commerce and banking sites, created to address the rise in Internet fraud that was eroding consumer confidence in online transactions. EV SSL certificates help verify a Web site owner though a comprehensive validation process. When consumers visit a site with an EV SSL certificate, the address bar turns green, representing a trust indicator that the owner of the site is who they purport to be. In addition a user can click on the company name for more information including where the company is located and incorporated. Efforts should be made to encourage EV SSL deployment by infrastructure providers for sites conducing commerce and collecting PII.

6. Account Verification / Passwords Management – User passwords and password re-set systems can often be exploited. Frequently cited reasons include the; use of names which can often be easily discovered by visiting a social networking site, infrequent changing of passwords and ineffective security challenge response questions used to re-set passwords. OTA has published recommendations to aid in creating such challenge questions, balancing security and usability, addressing the risks of readily discoverable information which might be posted or social engineering susceptible.[8] ISPs, carriers, hosters, email and infrastructure providers should complete a review of their password verification systems to help prevent account take overs and unauthorized access.

[7] http://www.washingtonpost.com/wp-dyn/content/article/2008/04/03/AR2008040304052.html
[8] https://otalliance.org/resources/index.html

OTA welcomes the opportunity to work with the FCC in the development of a collaborative and unified strategy to address the privacy, security and identify issues impacting consumer, business and government services. Working together we can help protect consumers and ensure the vitality and resiliency of the Internet and the internet economy.

Respectfully,

Craig D. Spiezle

Craig Spiezle
Executive Director
Online Trust Alliance

Cc: OTA Board & Steering Committee